Broadcom BACS for HP FlexFabric and StoreFabric Adapters User Guide

Abstract

This document is for the person who installs, administers, and troubleshoots servers and storage systems. HP assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.

Part Number: 741900-003
April 2014
Edition: 3

© Copyright 2013, 2014 Hewlett-Packard Development Company, Development Company, L.P.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

AMD is a trademark of Advanced Micro Devices, Inc. Intel is a trademark of Intel Corporation in the U.S. and other countries.

Microsoft®, Windows®, and Windows Server® are U.S. registered trademarks of Microsoft Corporation.

Contents

Introduction 5
BACS overview 5
Starting BACS 5
BACS interface on Microsoft Windows operating systems 5
Explorer View pane 5
Context View selector 6
Context View pane 6
Menu bar 6
Description pane 7
Installation overview 8
Introduction 8
Hardware requirements 8
Software requirements 8
Communication protocols 9
Installation summary 9
Installation summary for Microsoft Windows operating systems 9
Installation summary for Linux operating systems 10
Installing BACS components on Microsoft and Linux operating systems 12
WinRM installation steps 12
Basic configuration 12
User configuration 12
Configuring HTTP 12
Configuring HTTPS 13
Generating a self-signed certificate for Microsoft and Linux servers 14
Installing the management application 18
Installation on Microsoft Windows OS 18
Installing the BACS management client on a Microsoft Windows operating system 18
Configuring HTTP on Microsoft operating systems 18
Configuring HTTPS on Microsoft operating systems 19
Testing a client WinRM HTTPS/SSL connection 19
Installation on Linux OS 19
Downloading and unpacking HP SoftPaq 20
Installing OpenSSL and OpenPegasus 20
Installing WS-MAN and CimXML on Linux OS 21
Installing OpenPegasus from Inbox RPM for Red Hat 21
Installing OpenPegasus from Source for Red Hat and SuSE 21
Launching the application 29
Launching the GUI in Microsoft Windows OS 29
Launching the GUI in Linux OS 29
Closing the GUI in Microsoft Windows OS 29
Launching the CLI from Microsoft Windows OS 29
Launching the CLI from Linux OS 29
Closing the CLI 29

Configuration 30
Configuring preferences 30
Enabling or disabling the BACS tray icon 30
Setting Explorer View refresh time 30
Connecting to a host 30
Adding a local host 30
Adding a remote host 30
Managing the host 31
Information tab 31
Configuration tab 31
Managing the network adaptor 31
Viewing adapter information 32
Viewing resource information 32
Viewing hardware information 32
Configuring adapter parameters 33
Configuring multi-function parameters 33
Hardware and resource configuration wizard 33
Managing the Ethernet controller (port) 33
Viewing port level information 33
Viewing vital signs 34
Managing the LAN device 35
Viewing NDIS information 35
Viewing resource information 36
Viewing statistics 36
Viewing resource reservations 39
Changing the MTU size of iSCSI ports 39
Configuring the IP address for iSCSI offload 39
CLI commands 41
Configuring with the CLI utility 41
Support and other resources 42
Before you contact HP 42
HP contact information 42
Acronyms and abbreviations 43
Documentation feedback 46
Index 47

Introduction

BACS overview

BACS is an integrated utility that provides useful information about each network adapter installed in a system. BACS provides views of property values and traffic statistics for network objects. BACS also enables modification of property values. BASP functionality configures VLANs and runs within BACS systems that use at least one Broadcom-based network adapter.

Starting BACS

From the Control Panel, click **Broadcom Control Suite 4** to start the BACS. Or, click the BACS icon located in the taskbar at the bottom of the Windows desktop.

BACS interface on Microsoft Windows operating systems

The BACS Microsoft Windows interface contains the following regions:

- Explorer View pane
- Context View selector
- Context View pane
- Menu bar
- Description pane

The default configuration docks and pins the Explorer View pane on the left side of the main window, the Context View pane on the right, the Context View selector below the menu bar, and the Description pane below the Context View pane. Drag the splitter between any two panes to vary the pane size.

Explorer View pane

Dock and pin the Explorer View pane on the left side, right side, top, or bottom of the main window.

The Explorer View pane lists the objects that you can view, analyze, test, or configure using BACS. When you select an item from the Explorer View pane, the Context View pane displays the tabs with the information and options available for the item.

The organization and design of this panel presents the manageable objects in the same hierarchical manner as drivers and subcomponents. This simplifies the management of various elements of the adapters. The top level of the hierarchy is the Host container, which lists all hosts managed by BACS. Below the hosts are the installed network adapters, with the manageable elements such as physical port VBD, NDIS, FCoE, and iSCSI, below the adapters.

The icon next to each device in the Explorer View pane shows its status. An icon next to a device name that appears normal means the device is connected and working.

- **X** appears on the device icon to indicate the device is currently not connected to the network.
- **Greyed out** device icons indicate the device is currently disabled.

Context View selector

The Context View selector appears below the menu bar and includes the filter and tab categories. Expand or collapse the categories that appear on the tabs in the Context View pane. To display a category, select the box next to the category name.

Filter view

A multiple-host environment that uses different adapters and contains multiple configurable elements can be difficult to manage. Use the following view filters to increase device administration efficiency:

- All
- NDIS/L2NIC
- iSCSI
- FCoE
- iSCSI target
- FCoE target

Context View pane

The Context View pane displays all the parameters that you can view for the object selected in the Explorer View pane. The parameters are grouped by tabs and categories, depending on the parameter type. The available tabs are Information, Configuration, Diagnostics, and Statistics. Because the BACS interface is context-sensitive, only the parameters that apply to the selected object can be viewed or configured in the Context View pane.

Menu bar

The following options appear on the menu bar. Because the menu items are context-sensitive, not all items are available at all times.

File menu

Action menu

- **Add Host** adds the selected host.
- **Discover Hosts** discovers hosts.
- **Boot Configurations** configures the iSCSI boot parameters.
- **Remove Hosts** removes the selected host.
- **Remove All Hosts** removes all the hosts.
- **Refresh All** refreshes all the hosts.

View menu

- **Explorer View** displays and hides the Explorer View pane.
- **Tool Bar** displays and hides the tool bar.
- **Status Bar** displays and hides the status bar.
- **Broadcom Logo** displays and hides the logo on BACS to optimize the maximum viewable space.

Tools menu

Options configure BACS preferences.

iSCSI menu

- **Discovery Wizard** locates targets and helps to configure the HBA.
- **Manage Targets Wizard** manages targets.
- **Manage iSNS Servers** manages iSNS servers to allow discovery, management, and configuration of iSCSI devices.
- **Manage Discovery Portals** manages iSCSI discovery portals.

Discovery Wizard

The Discovery Wizard is available from the iSCSI menu. Follow the prompts in the wizard to discover iSCSI targets using the SendTargets method or the Internet iSNS server.

Manage iSNS Servers

The Manage iSNS Servers window is available from the iSCSI menu. Add or remove iSNS servers from this window.

Manage Discovery Portals

The Manage Discovery Portals window is available from the iSCSI menu. Add or remove iSCSI discovery portals from this window.

Boot Configuration Wizard

The Boot Configuration Wizard is available by right-clicking a port. Follow the prompts in the wizard to configure the iSCSI boot parameters.

Hardware and Resource Configuration Wizard

Use the Hardware and Resource Configuration Wizard to configure properties for hardware resources. Follow the prompts in the wizard to configure hardware resources. You can preview the configuration before committing the changes.

Description pane

The Description pane provides information, configuration instructions, and options for the selected parameter in the Context View pane.

Installation overview

Introduction

BACS management can be installed on both Microsoft Windows and Linux platforms.

The BACS installer package for the Microsoft Windows OS is based on Microsoft MSI installation technology. The Broadcom Windows CIM provides WS-MAN and WMI protocol support for client-server connections.

The Broadcom Linux CIM provides WS-MAN protocol and CimXML protocol support for client-server connections.

Hardware requirements

Systems that host BACS must meet the following hardware requirements:

- At least one of the following HP FlexFabric adapters:
  - HP FlexFabric 10Gb 2-port 534M Adapter
  - HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
  - HP FlexFabric 10Gb 2-port 534FLB Adapter
  - HP StoreFabric CN1100R 2-port CNA Adapter
  - HP FlexFabric 20Gb 2-port 630FLB Adapter
  - HP FlexFabric 20Gb 2-port 630M Adapter
- A single or multiprocessor HP ProLiant Gen8 system
- 128 MB of physical RAM to run the BACS4 GUI Management Application

  HP recommends 256 MB because less memory can severely affect performance.
- A video card capable of handling 256K colors and screen resolution of 800 x 600

  HP recommends 16K colors and 1024 x 768 resolution.
- At least 200 MB disk space

Software requirements

BACS is designed to run on the following Microsoft Windows platforms:

- Microsoft Windows Server 2012 64-bit, Intel 64, AMD 64
- Microsoft Windows Server 2008 32-bit, 64-bit Intel x86, Intel 64, AMD 64
- Microsoft Windows Server 2008 R2 64-bit, Intel 64, AMD 64

To use the SNMP management features, install the SNMP service. There is no other software requirement for Microsoft Windows. All required software components are included in the BACS4 GUI installer package and are installed as part of the installation process.

BACS is designed to run on the following Linux platforms:

- Red Hat Enterprise 5, 32-bit, 64-bit Intel x86, Intel 64, AMD 64
- Red Hat Enterprise 6, 32-bit, 64-bit Intel x86, Intel 64, AMD 64
- SuSE Enterprise, SLES, 10, 32-bit, 64-bit Intel x86, Intel 64, AMD 64
- SuSE Enterprise, SLES, 11, 32-bit, 64-bit Intel x86, Intel 64, AMD 64

The Linux OS requires specific software components. For more information, see "Installing BACS components on Microsoft and Linux operating systems (on page 12)."

Communication protocols

Broadcom provides the following communication protocols that are used to connect server and client systems:

- Microsoft Windows clients and servers can use WMI and WS-MAN/WinRM.

  Linux systems that connect to Microsoft Windows servers can use the WS-MAN/WinRM protocol to connect to the Microsoft Windows server.
- Linux clients and servers can use CimXML/Open Pegasus and WS-MAN/Open Pegasus.

  Microsoft Windows clients that connect to Linux servers can use the CimXML/Open Pegasus and WS-MAN/Open Pegasus protocols to connect to the Linux server.
- If Microsoft Windows and Linux clients both access Windows and Linux servers on a network, use the WS-MAN protocol.
- If Linux is the only OS installed on the servers, use the CimXML protocol.
- If the network only has Microsoft Windows clients and servers, use the WMI protocol. WMI does not require as much configuration as other protocols but is only supported on Microsoft Windows systems.

Installation summary

Install BACS on either, or both, Microsoft Windows and Linux operating systems.

Installation summary for Microsoft Windows operating systems

Microsoft Windows Server

Use the following items to install BACS on a Microsoft Windows Server. For the complete installation instructions, see "Installing BACS components on Microsoft and Linux operating systems (on page 12)."

To install BACS on a Microsoft Windows server:

1. Install WinRM software component on the server.
2. Perform Basic configuration on the server.
3. Perform User configuration on the server.
4. Perform HTTP configuration on the server.
5. Perform HTTPS configuration on the server.
   a. Generate a self-signed certificate for Microsoft Windows server.
   b. Install a self-signed certificate on a Microsoft Windows server.

6. Configure, and then test the WinRM listener on the server.
7. Perform additional configuration, if required, like firewall configuration on the server.
8. Install the BACS management application.

Microsoft Windows client

Use the following items to install BACS on a Microsoft Windows client. For the complete installation instructions, see "Installing BACS components on Microsoft and Linux operating systems (on page 12)."

To install BACS on a Microsoft Windows client:

1. If you plan to use HTTP with WS-MAN, perform HTTP configuration on a client.
2. If you plan to use HTTPS with WS-MAN, perform HTTPS configuration on a client.
3. Configure WinRM listener on a client.
4. Install the BACS client application on client systems.

The WMI protocol is only supported on Microsoft Windows OS. CimXML is not supported on Microsoft Windows OS.

BACS WMI on a Microsoft Windows server

Use the following items to install BACS WMI on a Microsoft Windows server. For the complete installation instructions, see "Setting up namespace security using WMI control (on page 26)."

To install BACS WMI on a Microsoft Windows server:

1. Set namespace security using WMI control.
2. Grant DCOM remote launch, and then activate permission for a user or group.
3. Perform special configuration, if necessary.
4. Follow the standard Microsoft Windows client installation steps to use WMI on a Microsoft Windows client.

Installation summary for Linux operating systems

Use the following items to install BACS on a Linux server. For the complete installation instructions, see "Installing BACS components on Microsoft and Linux operating systems (on page 12)."

Install the following items in the following order:

1. OpenSSL
2. Pegasus
3. `BRCM_CMPIProvider-x.x.x.rpm`
4. `BACS-x.x.x.rpm`

There are two installation options available with OpenPegasus–Inbox RPM or from source. The Inbox OpenPegasus is only available on Red Hat OS. For SLES11, the only available option is the source RPM. WS-MAN is not supported with the Inbox RPM. To use WS-MAN, install OpenPegasus from source.

To install BACS on a Linux server:

1. Install OpenPegasus on server from source RPM.
2. Start CIM Server on the server.
3. Configure OpenPegasus on server.
4. Install Broadcom CIM provider.

5. Perform additional configuration, if required, like firewall configuration.
6. Install the BACS client application on client systems, Microsoft Windows OS, or Linux.

Linux client

The following items are needed to install BACS on a Linux client. For the complete installation instructions, see "Installing BACS components on Microsoft and Linux operating systems (on page 12)."

To install BACS on a Linux client:

1. Install the following:
   a. OpenSSL
   b. Pegasus
   c. `BRCM_CMPIProvider-x.x.x.rpm`
   d. `BACS-x.x.x.rpm`
2. To use HTTPS with WS-MAN, perform HTTPS configuration on client.

   For HTTP, no special configuration is required on Linux client system. Only the BACS management application is required.
3. Install the BACS client application on client system.

BACS CimXML on a Linux server

Use the following items to install BACS CimXML on a Linux server. For the complete installation instructions, see "Installing BACS components on Microsoft and Linux operating systems (on page 12)." The installation steps for Linux server are similar to WS-MAN.

There are two installation options available with OpenPegasus–Inbox RPM or from source. The Inbox OpenPegasus is only available on Red Hat OS. For SLES11, the only available option is the source RPM. WS-MAN is not supported with the Inbox RPM. To use WS-MAN, install OpenPegasus from source.

To install BACS on a Linux server:

1. Install OpenPegasus on the server from Inbox RPM or from source RPM.
2. Start CIM Server on the server.
3. Configure OpenPegasus on the server.
4. Install the Broadcom CIM provider.
5. Perform additional configuration, if required, like firewall configuration.
6. Install the `sg3_utils` package, which is available in the Linux Distribution Package Repository. The package is required to query LUN information.
7. Install the BACS client application on client systems, Microsoft Windows OS, or Linux.
8. Follow the standard Linux client installation steps to use CimXML on a Linux client.

Installing BACS components on Microsoft and Linux operating systems

WinRM installation steps

WinRM 2.0 is pre-installed on Microsoft Windows 7 and Windows 2008 R2.

For Microsoft Windows 2008, install the Windows Management Framework Core that includes WinRM 2.0 and Windows Powershell 2.0. For more information, see the Microsoft website (http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=11829).

Basic configuration

The Microsoft Windows firewall must be enabled for WinRM to work properly.

To configure WinRM basic:

1. Configure the Microsoft Windows firewall.

   For detailed information about firewall configuration, see "Modifying Microsoft Windows Firewall rules (on page 16)."
2. Open a command prompt, and then run `winrm quickconfig`.

   The `winrm quickconfig` command enables remote management on the Microsoft Windows server.
3. Obtain the configuration information of the client service:

   ```
   winrm get winrm/config
   ```

   The output of this command is `RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD).`

   `BA` stands for BUILTIN\Administrators.

User configuration

A user account must be a member of the Microsoft Windows Administrators group on the local or remote computer to connect to WinRM. User accounts must also be added to the WinRM allowed connect list. Modify the root SDDL to include the user account or group. The SSDL ID for the account or group you want to add is required.

To add a user, for example with an SDDL ID of S-1-5-21-1866529496-2433358402-1775838904-1021:

```
winrm set winrm/config/Service
@{RootSDDL="O:NSG:BAD:P(A;GA;;;BA)(A;;GA;;;S-1-5-21-1866529496-2433358402-1775838904-1021)S:P(AU;FA;GA;;WD)(AU;SA;GWGX;;;WD)"}
```

Configuring HTTP

The default HTTP port for WinRM 2.0 is 5985.

To configure HTTP:

1. Select **Start→Run**, enter `gpedit.msc`, and then click **OK**.
2. Under Computer Configuration/Administrative Templates/Windows Components, select **Windows Remote Management**.
3. Under Windows Remote Management, select **WinRm Client**.
4. Under WinRM Client, double-click **Trusted Hosts**.
5. In the dialog, for TrustedHostsList, enter the hostnames of the clients.
6. If all clients are trusted, enter `*`, and then click **OK**.
7. Select **WinRM Service**.
8. Enable **Allow Basic Authentication**, and then click **OK**.
9. Enable **Allow unencrypted traffic**, and then click **OK**.
10. Close the `gpedit.msc` window.

To configure WinRM with default settings:

1. Open a command prompt, and then run the following command:
   ```
   winrm qc or winrm quickconfig
   ```
2. At the prompt `Make these changes[y/n]?`, enter `y`.

To verify the HTTP listener:

1. Open a command prompt, and then run one of the following commands:
   ```
   winrm enumerate winrm/confg/listener
   ```
   or
   ```
   winrm e winrm/config/Listener
   ```
2. Test the HTTP listener locally:
   ```
   winrm id
   ```

Configuring HTTPS

The HTTPS configuration process requires a self-signed certificate. Use BACS with an HTTPS/SSL connection to create and install a signed certificate on Microsoft Windows Server.

Be sure that Microsoft Windows and Linux clients are configured with the self-signed certificate. For more information, see "Configuring HTTPS on Microsoft operating systems (on page 19)" and "Configuring HTTPS on Linux systems (on page 25)."

Create a self-signed certificate on any Microsoft Windows or Linux server. Create the self-signed certificate on the computer running BACS, or copy the certificate from the server to the computer.

To use HTTPS with BACS:

1. Select **Start→Run**, enter `gpedit.msc`, and then click **OK**.
2. Under Computer Configuration/Administrative Templates/Windows Components, select **Windows Remote Management**.
3. Under Windows Remote Management, select **WinRm Client**.
4. Under WinRM client, double-click **Trusted Hosts**.
5. In the TrustedHostsList dialog, enter the client host names.
6. If all clients are trusted, enter `*`.

7. Select **WinRM Service,** and then enable **Allow Basic Authentication**.

Generating a self-signed certificate for Microsoft and Linux servers

Use Openssl to create a self-signed certificate. Openssl is available on both Microsoft Windows and Linux operating systems.

To create a self-signed certificate on Microsoft Windows:

1. Generate a private key:
   ```
   openssl genrsa -des3 -out server.key 1024
   ```
2. Enter a passphrase at the prompt. Be sure to record the passphrase.
3. Generate a CSR:
   ```
   openssl req -new -key server.key -out server.csr
   ```
4. At the prompt for a common name, enter the Microsoft Windows Server hostname or IP address.
5. Enter a value for all bolded parameters at the prompt for certificate information.

Remove a passphrase from a key

1. Run `cp server.key server.key.org`.
2. Run `openssl rsa -in server.key.org -out server.key`.

Generate a self-signed certificate

To generate a self-signed certificate that is valid for 365 days:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out
server.crt
```

The following example shows the output from the command:

```
Signature ok
subject=/C=US/ST=Texas/L=Houston/O=Hewlett-Packard/OU=Engineering/CN=MGM
TAPP- LAB3/emailAddress=
```

Verifying a self-signed certificate

To verify a self-signed certificate, run `openssl verify server.crt`.

The following example shows the output from the command:

```
server.crt:/C=US/ST=Texas/L=Houston/O=Hewlett-Packard/OU=Engineering/CN=
MGMTAPP- LAB3/emailAddress=
```

If an error message appears, such as `Error 18 at 0 depth lookup:self signed certificate`, ignore the message. The error indicates the certificate is self-signed.

Converting the certificate from crt to pkcs12 format

For Microsoft Windows Server, configure the certificate in the pkcs12 format.

To convert the certificate to pkcs:

1. Run `openssl pkcs12 -export -in server.crt -inkey server.key -out hostname.pfx`.
2. Enter a user name and password at the prompt.

Be sure to record the information to later import the certificate on a Microsoft Windows operating system.

3. Complete any additional steps as prompted.
4. Make a copy of `server.crt`, and then place the certificate file on the server where BACS is installed.

   To use a different computer to connect to the server running BACS, copy the same certificate to that computer.

For a Linux server, create the certificate with the .pem extension. It is unnecessary to use the `openssl` command to convert from .crt to .pem because only the file extension needs to change.

Transfer the certificate

If the certificate is on a system that does not host BACS, transfer the `hostname.pfx` to the Microsoft Windows server.

To transfer the certificate:

1. Select **Start→Run**, enter `mmc`, and then click **OK**.
2. From **File** menu, select the **Add/Remove** snap-in.
3. Select **Certificates**, and then click **Add**.
4. Select **Computer Account**.
5. Click **Next**, **Finish**, and then **OK**.
6. Expand **Certificates (Local Computer)**.
7. Expand **Personal**, and then right-click **Certificates**.
8. Select **All Tasks**, and then click **Import**.
9. Specify the certificate file location, and then select `hostname.pfx`.
10. At the prompt for a password for the private key, enter the same password as the self-signed certificate password.
11. Follow any instructions, select **defaults**, and then select **Continue**.

    The certificate shows as installed on the right side. The name is the `CN` selected during the certificate generation.
12. Right-click the certificate, and then select **Properties**.

    A dialog box states `Ensure that only Server Authentication is enabled as shown in the above dialog box.`
13. Expand **Trusted Root Certification Authorities**.
14. Expand **Certificates**.

    Repeat the steps in this procedure to import any additional certificates as needed.

To import a self-signed certificate on a client, see "Configuring HTTPS on Microsoft operating systems (on page 19)."

Configuring WinRM HTTPS/SSL

To create a WinRM listener:

1. Go to **Start→Run** menu, enter `mmc`, and then click **OK**.
2. From the **File** menu, select the **Add/Remove** snap-in.
3. Select **Certificates**, and then click **Add**.

4. Select **Computer Account**.
5. Click **Next**, **Finish**, and then **OK**.
6. Expand **Certificates (Local Computer)**.
7. Select the self-signed certificate from the personal store.

   If the certificate is created with a hostname, the hostname displays.
8. Double-click the hostname.
9. Select the **Details** tab.
10. Scroll down to, and then select, the **Thumbprint** field.
11. In the Details window select, and then copy, the thumbprint.
12. Return to the command prompt, and then run the following command:

    ```
    winrm create winrm/config/Listener?Address=*+Transport=HTTPS
    @{Hostname="<HostName or IPAddress>";CertificateThumbprint="<paste from
    the previous step and remove the spaces>"}
    ```

    If the certificate is generated using the HostName value, use the value. If the certificate is generated with the IP Address value, use the value.

    The command creates a listener on the HTTPS port (5986) with the network address of the server and the SelfSSL generated certificate.

Optionally, use `winrm` to create, modify, and then establish the https listener. WinRM listeners can be configured to use a variety of ports.

To verify the configuration:

1. To verify WinRM listeners, run `winrm e winrm/config/listener`.
2. To test HTTPS/SSL connections on a server, run `winrs -r:https://yourserver -u:username -p:password hostname`.

   If everything is configured correctly, the output of the command will print the server hostname name.
3. To verify the WinRM Service configuration, run `winrm get winrm/config/service`.

Additional configuration

Make any additional configuration changes in the Microsoft Windows firewall or with WinRM commands.

Modifying Microsoft Windows firewall rules

Use the following Microsoft Windows firewall modification guidelines to make any additional configuration changes.

To modify the Microsoft Windows firewall:

1. From the **Administrative Tools** menu, select **Microsoft Windows Firewall with Advanced Security**.
2. Right-click **Inbound Rules**, and then select **New Rule**.

   The new rule wizard appears.
3. Select **Port**, and then click **Next**.
4. On the Protocol and Ports screen, select **TCP**, and then enter the specific port, for example 5985 for HTTP or 5986 for HTTPS.
5. Click **Next**.
6. On the Action screen, select **Allow the connection**, and then click **Next**.

7. If the server is in a workgroup, select all three options in the Profile Settings, and then click **Next**.
8. Enter a name for the rule, and then click **Finish**.

   The new rule appears and is enabled as indicated by a green check box.

Useful WinRM commands

The following WinRM commands might be useful for additional configuration:

- Configure WinRM with default settings:

  ```
  winrm quickconfig or winrm qc
  ```

- Verify which service listeners are enabled and listening (including port and IP address):

  ```
  winrm enumerate winrm/config/Listener or winrm e winrm/config/Listener
  ```

- Verify the WinRM Service configuration:

  ```
  winrm get winrm/config/Service
  ```

- Delete an HTTPS listener:

  ```
  winrm delete winrm/config/Listener?Address=*+Transport=HTTPS winrm set
  winrm/config/service
  @{CertificateThumbprint="49598a83f844c5eee3ed379a391d41270da0b20b"}
  ```

Installing the management application

Installation on Microsoft Windows OS

Complete the following instructions to install BACS:

- Installing the BACS management client on a Microsoft Windows operating system (on page 18)
- Configuring HTTP on Microsoft operating systems (on page 18)
- Configuring HTTPS on Microsoft operating systems (on page 19)
- Testing a client WinRM HTTPS/SSL connection (on page 19)

Installing the BACS management client on a Microsoft Windows operating system

To install the BACS4 GUI/CLI management application on a Microsoft Windows system:

1. Download the Broadcom BACS4 installer package locally, and then extract the files.
2. Open the appropriate folder for the hardware platform.
3. Double-click `Setup.exe` to start the installation.
4. Click **Next**.
5. Accept the license agreement, and then click **Next**.
6. Select components:

   Control Suite is a GUI component. Select the option to install the GUI and CLI client on the host.

   SNMP installs a SNMP sub-agent that allows the SNMP manager to monitor Broadcom network adapters.

   CIM Provider presents the network adapter information to WMI-based management applications. Select the component on a host that has the installed Broadcom adapter that manages with the GUI client.
7. Click **Next**, **Next**, and then **Install**.
8. If a Windows security dialog box appears, select **Install this driver software anyway**.
9. Click **OK**, and then click **Finish**.

After installation, start the GUI from Microsoft Windows Start menu. For more information, see "Launching the application (on page 29)."

Configuring HTTP on Microsoft operating systems

To configure BACS HTTP:

1. Select **Start→Run**, enter `gpedit.msc`, and then click **OK**.
2. Under Computer Configuration/Administrative Templates/Windows Components, select **Windows Remote Management**.

3. Under **Windows Remote Management**, select **WinRm Client**.
4. Under WinRM Client, double-click **Trusted Hosts**.
5. In the dialog for TrustedHostsList, enter the hostnames of the clients.
6. If all clients are trusted, enter `*`.
7. Select **WinRM Service**.
8. Enable **Allow Basic Authentication**.
9. To test the connection, open a command prompt, and then run the following command:

   ```
   winrm id -remote:<remote machine Hostname or IP Address>
   ```

Configuring HTTPS on Microsoft operating systems

To configure BACS HTTPS:

1. Generate a self-signed certificate.

   Be sure to complete all steps. For more information, see "Generating a self-signed certificate for Microsoft and Linux servers (on page 14)."
2. Select **Start→Run**, and then type `mmc`.
3. Click **OK**.
4. Click **File→Menu**, and then select the **Add/Remove** snap-in.
5. Select **Certificates**, and then click **Add**.
6. Select **Computer Account**.
7. Click **Next**, **Finish**, and then **OK**.
8. Right-click **Trusted Root Certification Authorities**, and then select **All Tasks**.
9. Select **Import**, follow any instructions (for example, to provide the location of the exported `.pfx` file), and then select **Continue**.

Testing a client WinRM HTTPS/SSL connection

To retrieve the server operating system information:

```
winrm e wmi/root/cimv2/Win32_OperatingSystem-r:https://yourservername
-u:username -p:password –skipCAcheck
```

To retrieve the server WinRM identity information:

```
winrm id -r:https://yourservername -u:username -p:password-skipCAcheck
```

To enumerate windows services on a server:

```
winrm e wmicimv2/Win32_service -r:https://yourservername-u:username
-p:password -skipCAcheck
```

To avoid a `WSManFault` error, use the `–skipCAcheck` switch in the WinRM command lines because the certificate is self-generated and not imported on the client.

Installation on Linux OS

Complete the following instructions to install BACS:

- Downloading and unpacking HP SoftPaq (on page 20)

- Installing OpenSSL and OpenPegasus (on page 20)
- Installing WS-MAN and CimXML on Linux OS (on page 21)
- Installing OpenPegasus from Inbox RPM for Red Hat (on page 21)
- Installing OpenPegasus from Source for Red Hat and SuSE (on page 21)

Downloading and unpacking HP SoftPaq

1. Download, and then unpack the HP SoftPaq to a directory on the target computer.

   The SoftPaq is a .tgz file named by the SoftPaq Number.
2. Extract the files from the .tgz file:

   `tar -zxvf *.tgz`
3. (Optional) Delete the downloaded .tgz file.

Installing OpenSSL and OpenPegasus

To install OpenSSL and OpenPegasus:

1. To use SLES, download OpenSSL from the OpenSSL website (http://www.openssl.org/source/).
2. Download OpenPegasus from the OpenPegasus website (http://pegasus.isi.edu/downloads).
3. Obtain CMPIProvider and BACS from the NCDE builds.
4. Untar the OpenSSL package, and then compile OpenSSL and Pegasus.

   The OpenSSL package must be untarred because of the source code format.
5. To determine if the Linux version is missing anything required to compile the source and to create the makefile, open a command prompt, and then run the following command:

   `./config no_threads_fPIC`
6. Run `make` to build the package.
7. Run `make install` to install the package.
8. Untar the OpenPegasus package.
9. Check that the build environment is correctly defined to compile OpenPegasus:

   `vi /root/.bash_profile`

   For more information, see "Installing OpenPegasus from Source for Red Hat and SuSE (on page 21)."
10. Check that the OpenPegasus content is clean before compiling:

    `make clean`
11. To build the package, run `make`.
12. To install the package, run `make repository`.
13. Check that OpenPegasus is installed correctly in the Linux distribution:

    `cimcli`

    For more information, see the "Starting and stopping the CIM Server (on page 23)."
14. Configure OpenPegasus.

    For more information, see "Starting and stopping the CIM Server (on page 23)."
15. Install the Broadcom CIM Provider package:

    `rpm -i BRCM_CMPIProvider-x.x.x.rpm`

16. Configure the Linux firewall.

    For more information, see "Configuring the Linux firewall (on page 24)."

17. Configure HTTPS.

    For more information, see "Configuring HTTPS on Linux systems (on page 25)."

18. Install the BACS package:

    ```
    rpm –i BACS-x.x.x.rpm
    ```

19. When installation is complete, a BACS icon appears on the desktop.

    For more information about launching BACS, see "Launching the application (on page 29)."

Installing WS-MAN and CimXML on Linux OS

Install OpenPegasus from either of two sources: Inbox RPM or source RPM. Inbox OpenPegasus is only available on Red Hat OS. Source RPM is the only option available for SLES11.

WS-MAN is not supported with the Inbox RPM. To use WS-MAN, install OpenPegasus from source RPM.

Installing OpenPegasus from Inbox RPM for Red Hat

To install OpenPegasus on Linux Red Hat:

1. Locate the Inbox OpenPegasus rpm file named `tog-pegasus-<version>.<arch>.rpm`.
2. Run the following command:

   ```
   rpm -ivh tog-openpegasus-<version>.<arch>.rpm
   ```

3. Start Pegasus:

   ```
   /etc/init.d/tog-pegasus start
   ```

When complete, restart the Linux server, and then manually start the CIM Server. For more information, see "Starting and stopping the CIM Server (on page 23)." Be sure that client computers can connect to the BACS server, which is a known limitation of Red Hat v6.2 Inbox RPM.

Installing OpenPegasus from Source for Red Hat and SuSE

Download the OpenPegasus source file from the OpenPegasus website (http://www.openpegasus.org).

To use HTTPS to connect a client to the BACS server, be sure to install OpenSSL and libopenssl. The components are only necessary for HTTPS.

OpenPegasus variables

The following commands are the OpenPegasus variables.

Command	Details
`PEGASUS_ROOT`	The location of the Pegasus source tree
`PEGASUS_HOME`	The location of the executable repository Examples of executable files: • `$PEGASUS_HOME/bin` • `PEGASUS_HOME/lib` • `$PEGAUS_HOME/repository` • `$PEGASUS_HOME/mof subdirectories`

Command	Details
PATH	$PATH:$PEGASUS_HOME/bin
PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER	True
PEGASUS_CIM_SCHEMA	CIM222
PEGASUS_PLATFORM	For Linux 32 bit system: LINUX_IX86_GNU For Linux 64 bit systems: LINUX_X86_64_GNU
PEGASUS_HAS_SSL	Optional Set to true for HTTPS support.
PEGASUS_ENABLE_PROTOCOL_WSMAN	Optional Set to true for WSMAN protocol support.

OpenPegasus additional settings

The following command are additional OpenPegasus settings:

$PEGASUS_HOME needs to be set up in the shell environment.

$PEGASUS_HOME/bin needs to be appended to the $PATH environment.

The following command examples configure the settings:

```
export PEGASUS_PLATFORM="LINUX_X86_64_GNU"
export PEGASUS_CIM_SCHEMA="CIM222"
export PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER=true
export PEGASUS_ROOT="/share/pegasus-2.10-src"
export PEGASUS_HOME="/pegasus"
export PATH=$PATH:$PEGASUS_HOME/bin
```

For SSL support, add the following environment variable:

```
export PEGASUS_HAS_SSL=true
```

For WS-MAN Support, add the following environment variable:

```
export PEGASUS_ENABLE_PROTOCOL_WSMAN=true
```

CimXML and WSMAN use the same ports for HTTP and HTTPs, port 5989.

Add exports at the end of the .bash_profile. The file is located in the /root directory. If the environment variables are not set on a Linux system, run the following command:

```
source /root/.bash_profile
```

Building and installing OpenPegasus

To build and install OpenPegasus:

1. Navigate to the $PEGASUS_ROOT directory, which is the location of the OpenPegasus source root directory.
2. Run the following commands:

```
make clean
make
make repository
```

Whenever OpenPegasus is built from source, all configurations reset to default. To rebuild OpenPegasus, reconfigure the installation. For more information, see "Configuring OpenPegasus on a server (on page 23)."

Starting and stopping the CIM Server

To start CIM Server, run `cimserver` from a command prompt.

To stop the CIM Server, run `cimserver -s` from a command prompt.

Check if OpenPegasus is installed properly:

```
cimcli ei -n root/PG_Interop PG_ProviderModule
```

If the OpenPegasus installation is compiled from source, open the `PEGASUS_HOME directory` to start CIM Server, or CIM Server does not load the repository properly. For ease of use, set `PEGASUS_HOME` in the `.bash_profile` file.

Configuring OpenPegasus on a server

To configure OpenPegasus, first start CIM Server. Enter `cimserver` at the command prompt.

Use the following `cimconfig` commands and switches.

Command	**Details**
`cimconfig -l`	List all valid property names
`cimconfig -l -c`	List all valid property names and values
`cimconfig -g <property name>`	Query a particular property
`cimconfig -s <property name>=<value> -p`	Set a particular property
`cimconfig --help`	Find out more about the command

Stop and restart the CIM Server for the configuration changes to take effect.

For more information, see "Starting and stopping the CIM Server (on page 23)."

Enabling authentication

Before BACS launches, set the OpenPegasus properties to be sure that the Broadcom CIM Provider is configured correctly.

To set the OpenPegasus properties:

1. If CIM Server is not started, start CIM Server.

   For more information, see "Starting and stopping the CIM Server (on page 23)."

2. Run the following commands:

   ```
   cimconfig -s enableAuthentication=true -p
   cimconfig -s enableNamespaceAuthorization=false -p
   cimconfig -s httpAuthType=Basic -p
   cimconfig -s passwordFilePath=cimserver.passwd -p
   cimconfig -s forceProviderProcesses=false -p
   ```

3. To connect the root user remotely, run the following command:

   ```
   cimconfig -s enableRemotePrivilegedUserAccess=true -p
   ```

4. Because OpenPegasus authentication uses Linux system users, add the users to OpenPegasus:

   ```
   cimuser -a -u <username> -w <password>
   ```

Enabling HTTP

1. Start the CIM Server if the CIM Server is not already started.

   For more information, see "Starting and stopping the CIM Server (on page 23)."
2. (Optional) To set the HTTP port, run the following command:

   ```
   cimconfig -s httpPort=5988 -p
   ```

   The property is not available for Inbox OpenPegasus.
3. Enable an HTTP connection:

   ```
   cimconfig -s enableHttpConnection=true -p
   ```
4. Stop and restart the CIM Server:

   ```
   cimserver -s and cimserver
   ```

Enabling HTTPS

1. Start the CIM Server if the CIM Server not already started.

   For more information, see "Starting and stopping the CIM Server (on page 23)."
2. (Optional) To set the HTTPS port, run the following command:

   ```
   cimconfig -s httpsPort=5989 -p
   ```

   The property is not available for Inbox OpenPegasus.
3. Enable an HTTPS connection:

   ```
   cimconfig -s enableHttpsConnection=true -p
   ```
4. Stop and restart CIM Server:

   ```
   cimserver -s and cimserver
   ```

Installing Broadcom CIM provider

1. Be sure that OpenPegasus is installed properly.
2. Install the Broadcom CIM provider:

   ```
   % rpm -i BRCM_CMPIProvider-{version}.{arch}.rpm
   ```

Uninstalling Broadcom CIM provider

Run `% rpm -e BRCM_CMPIProvider.`

Configuring the Linux firewall

By default, CimXML over HTTP uses TCP and port number 5988, and CimXML over HTTPS uses TCP and port number 5989. Use the following instructions to open the ports, or other user-defined ports, on a Linux firewall.

Red Hat

To open ports in a Red Hat firewall:

1. Select **System→Administration→Firewall**.
2. Select **Other Ports**.
3. In the Port and Protocol dialog box, select **User Defined**.
4. In the **Port/Port Range** field, add the port number.

5. Add the protocol in the **Protocol** field, for example, **TCP** or **UDP**.
6. Click **Apply**.

SuSE

To open ports in a SuSE firewall:

1. Select **Computer→YaST**.
2. On the left pane, select **Security & Users**.
3. On the right pane, double-click **Firewall**.
4. On the left pane of the firewall dialog box, select **Custom Rules**.
5. On the right pane, select **Add**. A dialog box appears.
6. Enter the following information:
   - **Source Network**: **0/0**, which represents all interfaces
   - **Protocol**: **TCP**, or the appropriate protocol
   - **Destination Port**: <Port Number>, or <Range of Port Numbers>
   - **Source Port**: (leave blank)
7. Select **Next**, and then select **Finish**.

Installing the BACS management application

To install the BACS management application:

1. Download the latest BACS management application RPM package.
2. Install the RPM package:
   ```
   rpm -i BACS-{version}.{arch}.rpm
   ```

Uninstalling the BACS management application

Run the `rpm -e BACS` command.

Configuring HTTPS on Linux systems

Other than the BACS management application, no special software components are required on a Linux client system to use HTTP.

To use HTTPS on a Linux client, import a self-signed certificate.

Import a self-signed certificate

Linux distributions use the following directory for certificates:

```
SuSE uses /etc/ssl/certs
```

Red Hat can use one of two different directories:

```
/etc/ssl/certs
```

or

```
/etc/pki/tls/certs
```

If needed for the specific Linux distribution, determine which directory stores the certificates.

To import a self-signed certificate:

1. Copy the `hostname.pem` file into the certificate directory.

For more information, see "Generating a self-signed certificate for Microsoft and Linux servers (on page 14)."

2. Change directories to `/etc/ssl/certs`.
3. Create a hash value:

   ```
   openssl x509 -noout -hash -in hostname.pem
   ```

   The output looks like the following example:

   ```
   100940db
   ```
4. Create a symbolic link to the hash value:

   ```
   ln -s hostname.pem 100940db.0
   ```
5. If the installed OpenSSL version is earlier than 1.0.0d, perform the following steps:
   a. Build OpenSSL. Be sure that everything is linked statically.
   b. To build OpenSSL statically:

      ```
      /config no-shared
      make
      ```
   c. To create two hashes that point to the same certificate, change directories to `/etc/ssl/certs` for SuSE or `/etc/pki/tls/certs` for Red Hat.
   d. Run the following command:

      ```
      c_rehash
      ```
   e. Copy all `*.0` and any other symbolic files to a backup directory:

      ```
      cp -av *.0 <backup_directory>
      ```

      Be sure the `backup_directory` directory is empty before the files copy over.
   f. Make a backup of the `openssl` executable file that resides in the `/usr/bin` directory.
   g. Copy the `openssl` executable file from version 1.0.0d or later to the `/usr/bin` directory.
   h. Change directory to `/etc/ssl/certs/` or `/etc/pki/tls/certs`, depending on the Linux distribution, and then run the following command:

      ```
      c_rehash
      ```

      A new set of symbolic files is created.
   i. From the newly created backup directory, copy all the symbolic files back to the `/etc/ssl/certs`, or `/etc/pki/tls/certs` directory, depending on your Linux distribution.
   j. Change the directory to `/usr/bin`, and then delete the `openssl` executable file version 1.0.0d or later.
   k. Copy the original `openssl` executable, recently backed up, to the `/usr/bin` directory.
   l. Check that the certificate is installed correctly:

      ```
      # curl -v --capath /etc/ssl/certs https://Hostname or
      IPAddress:5986/wsman
      ```

      If the command fails, the certificate is not installed correctly. An error message provides information on any needed corrective action.

Setting up namespace security using WMI control

Manage namespace security with WMI control on a Microsoft Windows server.

To configure namespace security:

1. Start the WMI Control from the command prompt:

   `wmimgmt`

   On Microsoft Windows 9x or NT4 systems that have WMI installed, enter the following command instead:

   `wbemcntl.exe`

   Or, to access the WMI Control and the **Security** tab, do one of the following:

   - Right-click on **My Computer**, and then click **Manage**.

     For Microsoft Windows 2008, the Server Manager utility opens. WMI control is located in the left pane.
   - To open the Server Manager on Microsoft Windows 2012, select **Tools→Computer Management**.

     WMI Control is located on the left pane under **Services and Applications**. Right-click **WMI Control** to access the properties.
   - For all other versions of Microsoft Windows operating systems, double-click **Services and Applications**, and then double-click **WMI Control**.
2. Right-click **WMI Control**, and then click **Properties**.
3. In the WMI Control Properties dialog box, click the **Security** tab.

   A folder named `Root`, with a plus sign (+) next to it, appears.
4. Expand the tree, and then locate the namespace permissions that need configuration.
5. Click **Security**.

   A list of users and permissions displays. If the user account that needs modification is on that list, modify the permissions. If the user account is not on the list, click **Add** to add the user from the location, for example, a local machine or domain—wherever the account resides.
6. If a user account needs to access the namespace remotely, select **Allow** in the **Remote Enable** permission setting.

Granting DCOM remote launch and activate permissions

By default, in a Microsoft Windows domain environment, the domain administrator account has access rights to the WMI component used for the BACS management. No other special configuration is required.

In a large enterprise environment, however, users that need access to the machine running the BACS4 client GUI might not have the necessary rights to access the hosting machine by default. A network administrator must configure WMI security access on the machine hosting BACS4 to allow the appropriate users access.

To grant DCOM remote launch and activate permissions:

1. Select **Start→Run**, enter `dcomcnfg`, and then click **OK**.

   The Component Services dialog box opens.
2. Expand **Component→Services→Computers**, right-click **My Computer**, and then select **Properties**.
3. Click the **COM Security** tab.
4. In Launch and Activation Permissions, select **Edit Limits**.
5. If the required name or group does not appear in the groups or user names list, complete the following steps:

   a. Select **Add**.

   b. In the **Enter the object names to select** field, add the required name and group, and then click **OK**.

c. In the Launch Permission dialog box, select any user and group.

d. In the **Allow** column under the corresponding account permissions, select **Remote Launch**, **Remote Activation**, and then click **OK**.

   For more information, see the Microsoft website (http://msdn.microsoft.com/en-us/library/aa393266%28v=vs.85%29.aspx).

Special WMI configuration on other Microsoft Windows operating systems

Microsoft Windows XP and 2003 Server guest account configuration

For a Microsoft Windows XP Pro or Windows 2003 Server, make sure that remote log-on computers and accounts are not using the built-in guest account, sometimes referred to as a ForceGuest connection. By default, the built-in guest account is enabled on Microsoft Windows XP and 2003 Server systems not joined to a domain.

To prevent Microsoft Windows XP Pro and 2003 Server from using the guest account:

1. Select **Start**→**Run**, and then enter `secpol.msc`.
2. Click **OK**.
3. The Local Security Policy editor opens.
4. Expand the **Local Policies** node, and then select **Security Options**.
5. Scroll down to **Network access: Sharing and security model for local accounts**.
6. If **Network access: Sharing and security model for local accounts** is set to **Guest only**, change the setting to **Classic**, and then restart the computer.

Microsoft Windows Vista and Windows 7 Administrator group access

To allow all users in the Administrator group to connect the WMI namespace in Microsoft Windows Vista and 7, change the local account token filter policy as needed.

Launching the application

Launching the GUI in Microsoft Windows OS

To launch the BACS GUI, do one of the following:

- From the Program Menu, select **Start→All Programs→Broadcom→Broadcom Advanced Control Suite 4**.
- From the Control Panel, select **Start→Control Panel**, and then double-click **Broadcom Control Suite 4**.
- From the system tray, click **Broadcom Advanced Control Suite 4**.

  BACS might not appear in the Microsoft Windows Server 2008 system tray.

Launching the GUI in Linux OS

To launch the Linux BACS GUI, double-click the shortcut from the desktop.

Closing the GUI in Microsoft Windows OS

To close the BACS GUI, do one of the following:

- Click **File→Exit** on the BACS4 GUI window.
- Click the **X** button on the upper right corner of the BACS4 GUI window.

Launching the CLI from Microsoft Windows OS

To launch the BACS4 CLI on a Microsoft Windows operating system, double-click the `BACScli.exe` file installed in the `\Program Files\Broadcom\BACS` folder.

Launching the CLI from Linux OS

To launch the BACS4 CLI on a Linux client, execute the `BACScli` file installed in the `Opt/Broadcom/BACS` folder.

Closing the CLI

To close the CLI, do one of the following:

- Enter `q` at the prompt in the BACS4 CLI window.
- Click the **X** button on the upper right corner of the BACS4 CLI window.

Configuration

Configuring preferences

When the BACS program is installed, an icon in the Windows taskbar appears. Use the Options window to turn this icon on or off.

Enabling or disabling the BACS tray icon

1. From the Tools menu, select **Options**.
2. Select or clear **Enable BACSTray** (enabled by default).
3. Click **OK**.

Setting Explorer View refresh time

1. From the Tools menu, select **Options**.
2. Select **Auto** to set the Explorer View refresh time to 5 seconds. Otherwise, select **Custom** and select a time in seconds.
3. Click **OK**.

Connecting to a host

Add one or more Windows or Linux hosts for management from BACS.

Adding a local host

1. From the Action menu, click **Add Host**.

   For both Windows and Linux hosts, do not change the default settings. The User name and Password are not required while connecting to the local host.
2. Select **Persist** to save the information for this host.
3. Click **OK**. You can now use BACS to view information and manage the host.

Adding a remote host

1. From the Action menu, click **Add Host**.
2. Type the name of the remote host or the IP address in the Host box.
3. Select the protocol from the Protocol list. The protocol options for Windows are WMI, WSMan, or Try All. The protocol options for Linux are CimXML, WSMan, or Try All.

   The Try All option forces the GUI client to try all options.
4. Select the HTTP scheme, or select the HTTPS scheme for added security.
5. Type the host Port Number value if it is different than the default value of 5985.

6. Type the User name and Password.
7. Select **Persist** to save the information for this host. The host appears in the Explorer Pane the next time you open BACS, and you do not need to enter the host IP address or host name when connecting to the host.

   For security reasons, you must enter the User name and Password.
8. Click **OK**.

Managing the host

At the host level, you can view host information and configure parameters from the Information and Configuration tabs. To view host level information, select the host in the Explorer View pane, and then select the Information tab.

Information tab

Host information

- **Host Name** displays the name of the host.
- **OS Version Info** displays the operating system, including the version.
- **Platform** displays the hardware architecture platform (for example, 32-bit or 64-bit).

iSCSI initiator

Enable iSCSI on the host to view the iSCSI initiator section of the Information tab. The available information depends on the network adapter.

- **Name** displays the iSCSI initiator name in IQN format.
- **Portal List** displays all iSCSI portal IP addresses configured on the selected host.

To configure host-level parameters, select the host in the Explorer View pane, and then select the Configuration tab.

Configuration tab

System management

Chimney Offload State enables or disables chimney offload at the host level, rather than at the device level.

iSCSI initiator

Name displays the current IQN name. Click the IQN name to modify the host iSCSI initiator name.

Click **Apply** to save any changes.

Managing the network adaptor

The installed network adapters appear one level below the host in the hierarchical tree in the Explorer View pane. At the adapter level, you can view information and configure parameters from the Information and Configuration tabs.

Viewing adapter information

Select the network adapter in the Explorer View pane, and then select the Information tab to view adapter-level information.

Viewing resource information

You can view information about connections and other essential functions for the selected network adapter from the Resources section of the Information tab.

The available information depends on the network adapter.

- **Bus Type** is the type of input/output (I/O) interconnect used by the adapter.
- **Bridge** is the PCI-E to PCI-X bridge type. This information is only available for certain adapters.
- **Bridge Lanes** is the number of PCI-E lanes connected to the bridge. This information is only available for certain adapters.
- **Bridge Speed** indicates the clock speed on the PCI-E bus. This information is only available for certain adapters.
- **Slot Number** is the number of slots on the system board occupied by the adapter. This item is not available for PCI Express type adapters.
- **Bus Speed** indicates the bus clock signal frequency used by the adapter. This item is not available for PCI Express type adapters.
- **Bus Width** is the number of bits that the bus can transfer at a single time to and from the adapter. This item is not available for PCI Express type adapters.
- **Bus Number** indicates the number of the bus where the adapter is installed.
- **Device Number** is assigned to the adapter by the operating system.
- **Function Number** is the port number of the adapter. For a single-port adapter, the function number is 0. For a two-port adapter, the function number for the first port is 0, and the function number for the second port is 1.
- **Interrupt Request** interrupts the line number that is associated with the adapter. Valid numbers range from 2 to 25.
- **Memory Address** is the mapped address assigned to the adapter. This value can never be 0.
- **MSI Version** corresponds to the PCI specification. MSI corresponds to the PCI 2.2 specification that supports 32 messages and a single MSI address value. MSI-X corresponds to the PCI 3.0 specification that supports 2,048 messages and an independent message address for each message.

Viewing hardware information

You can view the Hardware section of the Information tab to display information about the hardware settings for the selected network adapter.

The available information depends on the network adapter. Examples include the following:

- **ASIC Version** is the chip version of the adapter.
- **Bootcode Version** of the boot code is only available for certain adapters.
- **Family Firmware Version** is a global firmware version that represents all firmware on the device.

- **Management Firmware** indicates the version installed on the system.
- **Vendor ID** indicates the vendor ID.
- **Device ID** indicates the adapter ID.
- **Subsystem Vendor ID** indicates the subsystem vendor ID.
- **Subsystem ID** indicates the subsystem ID.
- **External PHY Firmware Version** indicates the external PHY firmware version.

Configuring adapter parameters

Select the network adapter in the Explorer View pane, and then select the Configuration tab to configure adapter-level parameters.

Configuring multi-function parameters

Click **Configure** to configure multi-function parameters.

Hardware and resource configuration wizard

To modify device hardware and resource configurations with the Hardware and Resource Configuration Wizard:

1. Select a port to configure, and then click **Next**.
2. Configure the options:
   - **Flow Control** values are Auto, Tx Pause, Rx Pause, Tx/Rx pause, and Disable. The configuration is done at the port level and applies to all functions under the port. The flow control value is a default value for the port. The effective configuration can be different based on the switch port configuration and whether or not DCB/DCBX is enabled.
   - **Link Speed** configures the link speed.
   - **Ethernet/NDIS** enables Ethernet/NDIS capability.
   - **iSCSI** enables iSCSI functionality.
   - **FCoE** enables FCoE functionality.
3. Click **Apply** to commit changes to the system or click **Cancel**. Click **Finish** to save the changes and exit the wizard.

Managing the Ethernet controller (port)

To manage the Ethernet controller (port):

From BACS, group various traffic classes into a priority group, and then allocate bandwidth to each priority group.

Select the Ethernet controller from the object explorer panel to view the Information and Configuration tabs.

Viewing port level information

To view various types of information at the port level:

1. Select the Ethernet controller in the object explorer.
2. Select **PortX** (where X is either 0 or 1) below the adapter in the object explorer.

   Various components of the port are displayed below the port in the object explorer.
3. Click the plus sign icon next to the port to expand or collapse the tree below.
4. Select **Information tab** in the Context View Panel on the right side.

Viewing vital signs

The Vital Signs section of the Information tab has useful information about the installed network adapters, including the link status of the adapter and general network connectivity.

To view Vital Signs information for a network adapter, select the name of the adapter listed in the Explorer View pane, and then click the **Information** tab.

The available information depends on the specific network adapter.

- **MAC Address** is the physical MAC (media access control) address that is assigned to the adapter by the manufacturer. The physical address is never all 0s.
- **Permanent MAC Address** is the unique hardware address assigned to the network adapter.
- **iSCSI MAC Address** displays if an iSCSI network adapter is loaded onto the system.
- **IPv4 DHCP** enables using an IP address from a DHCP server.
- **IP Address** is associated with the adapter. If the IP address is all 0s, the associated driver has not been bound with Internet Protocol (IP).
- **IPv6 DHCP** enables using an IP address from a DHCP server.
- **IPv6 IP Address** is associated with the adapter.
- **IPv6 Scope Id** specifies the link where the destination is located to accommodate reusable, local-use (link-local) addresses. The Scope ID for site-local addresses specifies the site where the destination is located. The Scope ID is relative to the sending host.
- **IPv6 Flow Info** classifies traffic flows. If Flow Info equals zero, then the packets are not a part of any flow.
- **Default Gateway** is the network address of the gateway that will be used by the management firmware for packets destined for hosts external to the local network segment.
- **Link Status** provides status of the network link.
  - **Up** indicates the link is established.
  - **Down** indicates the link is not established.
- **Duplex** operates the adapter in the indicated duplex mode.
- **Speed** indicates the link speed of the adapter in megabits per second.
- **Offload Capabilities** indicates capabilities supported by the adapter. This information is only available for certain adapters.
  - **TOE** allows simultaneous operation of up to 1024 fully offloaded TCP connections for 1-Gbps network adapters and 1880 fully offloaded TCP connections for 10-Gbps network adapters to the hardware.
  - **iSCSI** indicates offload capability for block-level transfer of data.

- **LSO** prevents an upper level protocol such as TCP from breaking a large data packet into a series of smaller packets with headers appended to them.
- **CO** allows the TCP/IP/UDP checksums for send and receive traffic to be calculated by the adapter hardware rather than by the host CPU.

- **LiveLink IP Address** is the network address of the LiveLink enabled adapter.
- **Local Connection** identifies the module to which the blade server is attached.
  - **Chassis SW** is the chassis switch module.
  - **Chassis PHY** is the pass-through module.
  - **None** indicates that no modules are attached.
- **BASP State** provides information about the status of the BASP application. This information is displayed only when there is a team.

Managing the LAN device

The LAN function represents the Ethernet (NDIS) functionality available under the PCI Function. Select the FCoE object in the object explorer panel to view current values of various NDIS driver parameters, configure NDIS driver parameters, and view the attached FCoE targets and LUN information.

At the NDIS level, view and configure parameters from the Information and Configuration tabs.

Viewing NDIS information

Select the NDIS driver in the Explorer View pane, and then select the Information tab to view NDIS-level information.

The available information depends on the installed network adapter.

Viewing driver information, vital signs, and SR-IOV information

Driver Information

- **Driver Status** provides status of the adapter driver.
  - **Loaded** is the normal operating mode. The adapter driver has been loaded by Windows and is functioning.
  - **Not Loaded** indicates that the driver associated with the adapter has not been loaded by Windows.
  - **Information Not Available** indicates that the value is not obtainable from the driver that is associated with the adapter.
- **Driver Name** is the file name of the adapter driver.
- **Driver Version** is the current version of the adapter driver.
- **Driver Date** is the creation date of the adapter driver.

Vital Signs

- **IP Address** is the network address associated with the adapter. If the IP address is all 0s, the associated driver has not been bound with Internet IP.
- **IPv6 IP Address** is the IPv6 network address associated with the adapter.

- **MAC Address** is the physical media access control address that is assigned to the adapter by the manufacturer. The physical address is never all 0s.
- **Permanent MAC Address** is the unique hardware address assigned to the network adapter.
- **Offload Capabilities** are capabilities supported by the adapter. This information is only available for certain adapters.
  - **TOE** allows simultaneous operation of up to 1024 fully offloaded TCP connections for 1-Gbps network adapters and 1880 fully offloaded TCP connections for 10-Gbps network adapters to the hardware.
  - **iSCSI** indicates offload capability for block-level transfer of data.
  - **LSO** prevents an upper level protocol such as TCP from breaking a large data packet into a series of smaller packets with headers appended to them.
  - **CO** allows the TCP/IP/UDP checksums for send and receive traffic to be calculated by the adapter hardware rather than by the host CPU.

SR-IOV Switch Information

- **Number of HW Available** configures the number of available HW.
- **Number of Available VFs** configures the number of available VF.
- **Max VF Chains Per VFs** enters the number of maximum chains per VF.
- **VF Chains Pool Size** enters the pool size of VF chains.
- **Switch Friendly Name** enters the switch-friendly name.

Viewing resource information

The Resources section of the Information tab displays information about connections and other essential functions for the selected network adapter. The available information depends on the network adapter installed.

Resources

Bus Type is the input/output (I/O) interconnect type used by the adapter.

Viewing statistics

The information provided on the Statistics tab includes traffic statistics for different network adapters. Available statistics vary depending on the network adapter installed.

To view statistics information for any installed network adapter, click the name of the adapter listed in the Explorer View pane, and then click the **Statistics** tab. If any of the sections described below is not visible, select **Statistics** from the Context View tab, and then select the name of the missing section.

Click **Refresh** to access the most recent values for each statistic. Click **Reset** to change all values to zero for the current BACS session.

General Statistics

General Statistics show the transmitted and received statistics to and from the adapter.

- **Frames Tx OK** is a count of the frames that were successfully transmitted. This counter is incremented when the transmit status is reported as Transmit OK.

- **Frames Rx OK** is a count of the frames that were successfully received. This does not include frames received with frame-too-long, frame check sequence (FCS), length, or alignment errors, nor frames lost due to internal MAC sublayer errors. This counter is incremented when the receive status is reported as Receive OK.
- **Directed Frames Tx** is a count of directed data frames that were successfully transmitted.
- **Multicast Frames Tx** is a count of frames that were successfully transmitted (as indicated by the status value Transmit OK) to a group destination address other than a broadcast address.
- **Broadcast Frames Tx** is a count of frames that were successfully transmitted (as indicated by the transmit status Transmit OK) to the broadcast address. Frames transmitted to multicast addresses are not broadcast frames and are excluded.
- **Directed Frames Rx** is a count of directed data frames that were successfully received.
- **Multicast Frames Rx** is a count of frames that were successfully received and are directed to an active non-broadcast group address. This does not include frames received with frame-too-long, FCS, length, or alignment errors, nor frames lost because of internal MAC sublayer errors. This counter is incremented as indicated by the Receive OK status.
- **Broadcast Frames Rx** is a count of frames that were successfully received and are directed to a broadcast group address. This count does not include frames received with frame-too-long, FCS, length, or alignment errors, nor frames lost because of internal MAC sublayer errors. This counter is incremented as indicated by the Receive OK status.
- **Frames Rx with CRC Error** is the number of frames received with CRC errors.
- **Initiator Login Statistics** is an iSCSI login that enables a connection for iSCSI use between the initiator and the target and is used to authenticate parties, negotiate the session's parameters, open security association protocol, and mark the connection as belonging to an iSCSI session.
- **Login Accept Responses** is the number of login requests accepted by the target.
- **Login other failed Responses** is the number of login requests that were not accepted by the target.
- **Login Redirect Responses** is the number of responses that required further action by the initiator.
- **Login Authentication Failed Responses** is the number of login requests that failed due to party authentication failure.
- **Login target authentication failure** is the number of instances where the login could not authenticate the target.
- **Login target negotiation failure** is the number of instances where the login could not negotiate the sessions parameters.
- **Normal logout command PDU** is the number of normal logout commands issued by the initiator to remove a connection from a session or to close a session.
- **Other logout command PDU** is the number of logout commands issued by the initiator for reasons other than to remove a connection from a session or to close a session.
- **Local Initiator login failures** is the number of login failures likely caused by the initiator.
- **Initiator Instance Statistics** are statistics that pertain to all sessions.
- **Session digest errors** is the number of sessions with errors due to an invalid payload or header.
- **Session connection timeout error** is the number of sessions that were terminated due to any of the many timeout errors.

- **Session format error** is the number of sessions with errors due to inconsistent fields, reserved fields that are not 0, non-existent LUNs, and so forth.
- **Sessions failed** is the number of failed sessions.

Custom statistics

Total Offload iSCSI Connections is the total number of offloaded iSCSI connections.

Session Statistics

The statistics in this area only pertain to the named session.

- **Session Name** is the name used for the session between the initiator and the target.
- **Session Id** is the identifier used for the session between the initiator and the target.
- **Bytes sent** is the number of bytes sent for the named session.
- **Bytes received** is the number of bytes received for the named session.
- **PDU sent** is the number of iSCSI PDUs sent for the named session.
- **PDU received** is the number of iSCSI PDUs received for the named session.
- **Digest errors** is the number of errors due to an invalid payload or header for the named session.
- **Connection Timeout errors** is the number of connection timeout errors for the named session.
- **Format errors** is the number of errors due to inconsistent fields, reserved fields not 0, non-existent LUN, and so on for the named session.

IEEE 802.3 Statistics

- **Frames Rx with Alignment Error** provides a count of the frames that were not an integral number of octets in length and do not pass the FCS check. This counter is incremented when the receive status is reported as Alignment Error.
- **Frames Tx with one Collision** provides a count of the frames that were involved in a single collision and were subsequently transmitted successfully. This counter is incremented when the result of a transmission is reported as Transmit OK, and the attempt value is 2.
- **Frames Tx with more than one Collision** provides a count of the frames that were involved in more than one collision and were subsequently transmitted successfully. This counter is incremented when the transmit status is reported as Transmit OK, and the value of the attempts variable is greater than 2 and less than or equal to the attempt limit.
- **Frames Tx after Deferral** provides a count of the frames that were delayed being transmitted on the first attempt because the medium was busy. The frames involved in any collision are not counted.

Custom Statistics

Custom statistics are available only for certain enabled network adapters.

- **Out of Recv** provides the number of times the adapter ran out of Receive Buffer Descriptors. This information is only available for certain adapters.
- **Frames size less than 64-byte with bad FCS** provides the number of frames with a size less than 64 bytes with bad FCS.
- **MAC Rx w/ Pause Command and Length = 0** provides MAC control frames with the pause command and a length equal to 0.
- **MAC Rx w/ Pause Command and Length greater than 0** provides MAC control frames with the pause command and a length greater than 0.

- **MAC Rx w/ no Pause Command** enables MAC control frames with no pause command.
- **MAC Sent X-on** indicates that MAC Transmit with X-on is on.
- **MAC Sent X-off** indicates that MAC Transmit with X-on is off.
- **Large Send Offload Transmit Requests** is the number of times the adapter was requested to transmit a packet performing TCP segmentation.
- **Total Offload TCP Connections** is the total number of offloaded TCP connections.
- **SR-IOV Switch Statistics** shows the statistics for SR-IOV switches.
- **Num of Active VFs** shows the number of active VF.

Viewing resource reservations

Resource Reservation information is only available for certain adapters and VBD drivers. Not all offload technologies are available with all adapters.

The Resource Reservations section shows the number of connections allocated to an offload technology.

TOE and iSCSI

TOE and iSCSI can only be configured on certain adapters and require a license key. License keys are preprogrammed in the hardware.

- TOE enables accelerating TCP over 2.5 GbE and 10 GbE.
- iSCSI offload enables accelerating network storage access featuring centralized boot functionality (iSCSI boot).

The number of unlicensed resources and unallocated resources is also viewable.

To view resource reservations:

1. Click the name of the system device in the Explorer View pane.
2. From the Resource Reservations section, select the property you want to set.
   - Click **Apply** to confirm the changes to all properties.
   - Click **Reset** to return the properties to the original values.

Changing the MTU size of iSCSI ports

The iSCSI Management section of the Configurations tab changes the MTU of the iSCSI ports.

To change the MTU size of iSCSI ports:

1. Click the name of the Broadcom iSCSI device in the SCSI controller section of the Explorer View pane.
2. Enter the MTU size in the Value column.
3. Click **Apply** to save the settings or click **Reset** to revert to the previous settings.

Configuring the IP address for iSCSI offload

The iSCSI Management section of the Configurations tab sets the IP address of the iSCSI HBA when using iSCSI protocol to offload network processing from the CPU to a Broadcom-based network adapter. This procedure does not apply to iSCSI-booted adapters.

To set the IP address of the iSCSI HBA for iSCSI offload:

1. Click the name of the iSCSI device in the SCSI controller section of the Explorer View pane.
2. To set the IP address, do one of the following:
   - For IPv4 DHCP and IPv6 DHCP protocols, select **Enable** to set the IP address dynamically using a DHCP server (not available for iSCSI booted adapters).
   - For other protocols, select **Disable** to set the IP address using a static IP address.
3. Enter values for the IP Address, Subnet Mask, and Default Gateway.
4. Configure the VLAN ID for the iSCSI HBA by entering a number for VLAN ID. The value must be between 0 and 4094.
5. After the configurations are complete, click **Apply** to save the settings. Or, click **Reset** to revert to the previous settings.

CLI commands

Configuring with the CLI utility

An alternate method to BACS for configuring network adapters is BACSCLI, a utility that enables you to view information and configure network adapters using a console in either a non-interactive command line interface (CLI) mode or an interactive mode. BACSCLI provides information about each network adapter and enables modification of property values.

For a complete list of commands and examples, see the BACSCLI ReadMe text file available with the installation.

Supported operating systems

BACSCLI is supported on the following operating systems:

- Windows Server 2008 (including Server Core)
- Windows Server 2008 R2 (including Server Core)
- Windows Server 2012 (including Server Core)
- SuSE Linux Enterprise Server(SLES) 11 32 and 64 bit
- Redhat Enterprise Linux Redhat 5 32 and 64 bit
- Redhat Enterprise Linux Redhat 6 32 and 64 bit

Installation

BACSCLI is installed when BACS is installed with the installer.

Support and other resources

Before you contact HP

Be sure to have the following information available before you call HP:

- Active Health System log (HP ProLiant Gen8 or later products)

  Download and have available an Active Health System log for 3 days before the failure was detected. For more information, see the *HP iLO 4 User Guide* or *HP Intelligent Provisioning User Guide* on the HP website (http://www.hp.com/go/ilo/docs).

- Onboard Administrator SHOW ALL report (for HP BladeSystem products only)

  For more information on obtaining the Onboard Administrator SHOW ALL report, see the HP website (http://www.hp.com/go/OAlog).

- Technical support registration number (if applicable)
- Product serial number
- Product model name and number
- Product identification number
- Applicable error messages
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level

HP contact information

For United States and worldwide contact information, see the Contact HP website (http://www.hp.com/go/assistance).

In the United States:

- To contact HP by phone, call 1-800-334-5144. For continuous quality improvement, calls may be recorded or monitored.
- If you have purchased a Care Pack (service upgrade), see the Support & Drivers website (http://www8.hp.com/us/en/support-drivers.html). If the problem cannot be resolved at the website, call 1-800-633-3600. For more information about Care Packs, see the HP website (http://pro-aq-sama.houston.hp.com/services/cache/10950-0-0-225-121.html).

Acronyms and abbreviations

BACS

Broadcom Advanced Control Suite

BACSCLI

Broadcom Advanced Control Suite command line interface

BASP

Broadcom Advanced Server Program

CIM

common information model

CNA

Converged Network Adaptor

CO

Checksum Offload.

CRC

cyclic redundant checks

CSR

certificate signing request

DCOM

Distributed Component Object Model

DHCP

Dynamic Host Configuration Protocol

FCoE

Fibre Channel over Ethernet

FCS

Frame Check Sequence

HBA

host bus adapter

IQN

iSCSI qualified name

iSCSI

Internet Small Computer System Interface

iSNS

Internet Storage Name Service

LSO

large send offload

LUN

logical unit number

MAC

Media Access Control

MTU

maximum transmission unit

NDIS

network driver interface specification

PCI

payment card industry

PCIe

Peripheral Component Interconnect Express

PDU

protocol data unit

SDDL

Security Descriptor Definition Language

SLES

SUSE Linux Enterprise Server

SR-IOV

Single root I/O Virtualization

SSL

Secure Sockets Layer

TOE

TCP/IP Offload Engine

UDP

User Datagram Protocol

VF

SR-IOV virtual function

VF

virtual bus driver

VLAN

virtual local-area network

WinRM

Windows Remote Management

WMI

Windows Management Interface

WS-MAN

Web Service Management

Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (mailto:docsfeedback@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.

Index

A

adapter settings 32, 33
additional configuration 16

B

BACS communication protocols 8
BACS hardware requirements 8
BACS installation 8, 18
BACS installation procedure 12
BACS interface on Microsoft systems 5
BACS introduction 8, 9
BACS management application, installing 25
BACS management application, uninstalling 25
BACS software requirements 8
BACS, closing CLI 29
BACS, closing GUI 29
BACS, installing management client on Microsoft systems 18
BACS, launching CLI in Windows 29
BACS, launching GUI 29
BACS, launching GUI in Linux 29
BACS, launching the GUI in Linux 29
BACS, launching the GUI in Microsoft Windows 29
BACS, Linux installation 10, 19
BACS, Microsoft Windows installation 9, 18
boot configurations 7
Broadcom CIM provider, installing 24
Broadcom CIM provider, uninstalling 24

C

certificates 14
certificates, converting to pkcs12 format 14
certificates, generating 14
certificates, generating self-signed 14
certificates, verifying 14
CIM server, starting and stopping 23
CLI commands 41
CLI, accessing 41
communication protocols 9
configuration 7, 30
Configuration tab 31, 33
configuration, hardware 7

D

DCOM, granting remote launch and activate permissions 27
destination site 7
DHCP server 34
discovery protocols 5, 6, 7, 30, 31, 33
drivers 35

E

enabling authentication 23
enabling HTTP 24
enabling HTTPS 24

H

host connections 30
hosts, adding 30
hosts, managing 31
HP SoftPaq 20
HP SoftPaq, downloading and unpacking 20
HTTP, configuring 12
HTTP, configuring on Microsoft systems 18
HTTPS, configuring 13
HTTPS, configuring on Microsoft systems 19

I

Information tab 31, 32, 33, 34, 35
installation 8
installing WS-MAN and CimXML on Linux 21
IP address assignment 39
iSCSI boot targets 33, 35, 41
iSCSI initiator 31, 36
iSCSI offload 7, 34, 36, 39

L

LAN 35
Linux, configuring firewall 24
Linux, configuring HTTPS 25

M

maximum transmission unit (MTU) 39

menu bar 6
Microsoft iSCSI initiator software 31, 36
Microsoft Windows Firewall 16
Microsoft Windows Firewall, modifying 16
Microsoft Windows Server 2008 41
Microsoft Windows Server 2012 41

O

OpenPegasus variables 21
OpenPegasus, additional settings 22
OpenPegasus, building and installing 22
OpenPegasus, configuring on a server 23
OpenPegasus, installing from Inbox RPM for Red Hat 21
OpenPegasus, installing from source for Red Hat and SuSE 21
OpenSSL and OpenPegasus, installation 20
overview 5

P

passphrase, removing from key 14
preferences 30

R

refreshing data 30
resources 33, 36, 39, 42

S

setting up namespace security using WMI control 26
startup, BACS 5
statistics 36
support 42
supported operating systems 41

T

technical support 42
tray id switch 30, 34
tree navigation 31

W

WIM image 34
WinRM basic configuration 12
WinRM installation overview 12
WinRM user configuration 12
WinRM, test a client WinRM HTTPS/SSL connection 15, 19
WinRM, useful commands 17
WMI, special configuration on other Microsoft systems 28